Міністерство освіти і науки України НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

# Принципи роботи технології блокчейн та її властивості

## Текстова частина до курсової роботи за спеціальністю „Інженерія програмного забезпечення” 121

Керівник курсової роботи

Невмержицький Є. І.

*(підпис)*

“____” _____ 2021 р.

Виконала студентка

Волошенюк І. М.

“____” _____ 2021 р.

Київ 2021

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»
Кафедра інформатики факультету інформатики

ЗАТВЕРДЖУЮ
Зав.кафедри інформатики,

Доцент., к. ф.-м. н. С.С.Гороховський (підпис)

„____”_____2021 р.

**ІНДИВІДУАЛЬНЕ ЗАВДАННЯ**

на курсову роботу

студентці Волошенюк Ірині Михайлівні факультету інформатики 3-го курсу
ТЕМА Принципи роботи технології блокчейн та її властивості

Зміст ТЧ до курсової роботи:

1. Індивідуальне завдання
2. Календарний план
3. Анотація
4. Вступ
5. Принципи і особливості технології блокчейн
6. Поняття та види консенсусу
7. Види криптовалют, їх задачі, характеристики, функції і властивості
8. Порівняння криптовалют з фіатними грошима
9. Розробка криптовалюти та застосунка для зберігання і купівлі NFT токенів
10. Висновки
11. Список використаних джерел

Дата видачі “___” _____ 2021 р. Керівник Невмержицький Є. І. (підпис)

Завдання отримала Волошенюк І. М. (підпис)

**Тема:** Принципи роботи технології блокчейн та її властивості

Календарний план виконання роботи:

| № п/п | Назва етапу курсової роботи | Термін виконання етапу | Примітка |
|---|---|---|---|
| 1. | Отримання теми курсової роботи. | 15.10.2020 | |
| 2. | Огляд технології блокчейн | 15.11.2020 | |
| 3. | Написання основної частини | 20.03.2021 | |
| 4. | Розробка криптовалюти та застосунку для зберігання і купівлі NFT токенів | 20.04.2021 | |
| 5. | Завершення написання текстової частини курсової | 25.04.2021 | |
| 6. | Корегування роботи згідно із зауваженнями керівника | 02.05.2021 | |
| 7. | Створення презентації | 15.05.2021 | |

Студенту Волошенюк І. М. (підпис)

Керівник Невмержицький Є. І. (підпис)

“___” _____ 2021 р

# АНОТАЦІЯ

У курсовій роботі було проведено дослідження технології блокчейн. Зокрема, було описано та проаналізовано поняття криптовалют. На основі виділених характеристик було проведено порівняння з фіатними грошима.

Завдяки отриманим знанням, було розроблено власну криптовалюту на платформі Ethereum та веб-застосунок для роботи з NFT токенами на основі Node.js та React.

Ключові слова: блокчейн, децентралізована мережа, майнінг, консенсус, криптовалюта, токен, Ethereum.

# ЗМІСТ

# ПЕРЕЛІК ПРИЙНЯТИХ ТЕРМІНІВ І СКОРОЧЕНЬ

**PoW** – англ. “Proof-of-Work”.

**PoS** – англ. “Proof-of-Stake”.

**DPoW** – англ. “Delegated Proof-of- Stake”.

**PoC** – англ. “Proof-of-Capacity”.

**PoS** – англ. “Proof-of-Space”.

**PoST** – англ. “Proof-of-Space-Time”.

**PoA** – англ. “Proof-of-Activity”.

**IDE** – англ. “Integrated Development Environment”.

# Вступ

Технологія блокчейн, створена як розподілений реєстр для збереження важливої інформації з гарантованою достовірністю, стала фундаментом для створення аналога державних грошей – криптовалют. Саме після створення першої криптовалюти інтерес до даної технології почав невпинно зростати. Наразі, технологія блокчейн також широко використовується для смарт-контрактів, ідентифікації особистості, фінансових сервісів та цифровізації активів.

Недовіра до централізованої банківської системи, викликана економічними кризами або невдалою монетарною політикою, спонукає людей шукати альтернативні засоби для накопичення та розрахунку. Відповідно, це призводить до зростання популярності криптовалют. За довгий час свого існування криптовалюти змогли зарекомендувати себе як безпечний та надійний аналог державним валютам, завдяки своїй прозорості та надійності, обумовленої використанням блокчейну. Зі зростанням популярності криптовалют, підвищується їхня ліквідність та капіталізація, що також слугує активному розвитку технології блокчейн.

Об’єктами нашого дослідження є технологія блокчейн та криптовалюти.

Предметом дослідження є принципи технології блокчейн, структура та процес створення блоку у мережі блокчейн, поняття та види консенсусу, криптовалюти (класифікація, задачі, характеристики, функції і властивості) та їхнє порівняння з фіатними валютами.

Мета даної курсової роботи – огляд технології блокчейн та криптовалют, а також розробка власної криптовалюти та застосунку для зберігання і купівлі NFT токенів.

У ході роботи описано ключові принципи технології блокчейн. Особливості її реалізації розглядаються на прикладі криптовалют, а саме Bitcoin. Також

розкриваються переваги технології порівняно з консолідованим збереженням даних.

Наступним досліджується поняття консенсусу та описуються найбільш популярні або цікаві, з точки зору принципів роботи, види. Опис кожного виду консенсусу містить інформацію про принцип його роботи, енергоефективність, переваги та недоліки, породжені його функціональними особливостями. У тексті курсової роботи також опосередковано розкривається роль учасників системи в її функціонуванні та розвитку.

Тема криптовалют розглядається з погляду п’яти ключових понять: види, задачі, характеристики, функції і властивості. Оскільки, криптовалюти є різновидом цифрових валют, то перелік функцій і властивостей є аналогічним як і для інших грошей. З огляду на це, особлива увага приділяється тому наскільки криптовалюти задовольняють ту чи іншу функцію або властивість.

Наступним розділом є порівняння криптовалют та фіатних грошей. Співставляються їхні переваги та недоліки. Описуються відмінності, обумовлені як особливостями технологій, які лежать в їх основі, так і рисами закладеними творцями.

# 1. Принципи і особливості технології блокчейн

## 1.1 Основні принципи технології блокчейн

Технологія блокчейн виникла задовго для появи першої криптовалюти. Вона була розроблена у 1991 році Стюартом Хабертом і У. Скотт Шторнетом, щоб унеможливити підробку документів.

Блокчейн - це технологія, яка полягає в записі інформації послідовно в блоки. Блоки утворюють ланцюг, де кожен наступний елемент містить інформацію про попередній. Такий підхід дозволяє гарантувати, що жоден запис не було модифіковано чи видалено.

Кожен блок в ланцюзі блокчейн має власну хеш-суму. Саме вона забезпечує зворотній зв’язок блоків і унеможливлює підробку інформації. Хеш-сума являє собою результат певної математичної функції над усією інформацією в блоці і хеш-сумою попереднього (батьківського) блоку.

При зміні будь-якої інформації, яка міститься в блоці, хеш-сума теж зміниться. Кожен блок, окрім першого, містить хеш-суму батьківського блоку. Тому при зміні одного блоку, весь ланцюг перестає бути дійсним. Для того, щоб інші учасники мережі не помітили змін, необхідно перерахувати хеш-суму всіх наступних блоків. Це можливо лише за умови, коли більше 50% системи належать або є у змові зі зловмисником. Такі атаки мають назву “51% атака”. Принципи роботи сучасних блокчейн платформ роблять учасників зацікавленими у надійності системи. Надійність старих мереж (в тому числі Біткоїна) забезпечується за рахунок дуже складних обчислень. Таким чином, дана атака є малоймовірною або економічно невигідною. [1]

Перший блок в ланцюзі називається генезис-блоком. Оскільки, він не містить хеш-суму попереднього блоку, генезис-блок не використовується для запису інформації. Криптовалюта, що містить на ньому, не може бути переказана на жоден

гаманець. На його створення витрачається значно більше часу, ніж на створення всіх подальших. Наприклад, генезис-блок Біткоїна створювався 6 днів, на противагу 10 хвилин для звичайного.

Технологія блокчейн передбачає, що у блока може бути лише один батько та безліч нащадків. Таке відгалуження від основного ланцюга називається форк (fork). Форк створюється для запису блоків за зміненими правилами. Це може бути зроблено задля створення нової мережі або як спроба атаки на систему (наприклад, “nothing at stake”). [2, с. 163]

Для доступу до власних даних або криптовалюти використовують пару публічного і приватного ключів. Кожна така пара є унікальною і створюється за допомогою криптографії. Публічний ключ виступає у ролі гаманця для криптовалюти. Приватний ключ відомий лише власнику і при його втраті, доступ до рахунку або іншої інформації буде неможливо відновити. [2, с. 61-62]

## 1.2 Структура блоків

Блок складається з заголовку та записів (наприклад, транзакцій). Для криптовалют використовують блоки, до вмісту яких також входить адреса гаманця майнера, який створив його. Кожен блок має однаковий фіксований розмір.

Розглянемо вміст блоку детальніше на прикладі Біткоїна. Блок має розмір 1Мб. Заголовок містить в собі 3 типи інформації: посилання на попередній блок, дані для майнінгу та корінь дерева Меркля. Друга група даних складається зі значення складності алгоритму консенсусу для даного блоку, мітки часу (timestamp) - приблизного часу створення, та нонса (nonce) - лічильника. Дерева Меркля використовуються для ефективного хешування вмісту блока. Сумарний розмір заголовка складає 80 байтів. Решту місця в блоці займає близько 1900 транзакцій, по 400 байтів кожна. [2, с. 164]

## 1.3 Додавання блоків

Після того, як вміст одного блоку заповнився, необхідно створити наступний. Блокчейн – це розподілена система, яка не має централізованого управління, тому учасникам мережі необхідно самостійно створювати нові блоки. Для цього потрібно прорахувати хеш-суму попереднього блоку. Отриманий результат верифікують інші учасники мережі.

У випадку криптовалют, процес додавання нових блоків називається майнінгом. Залежно від платформи, механізм майнінгу може відрізнятись. У загальному випадку, майнери завантажують на свої комп'ютери частину розподіленої бази даних. Потім, на основі даних попереднього блоку, обраховується хеш-сума. Перший майнер, який обчислив правильний хеш, отримує комісійну винагороду. Після верифікації результату іншими учасниками мережі, новий блок додається до ланцюга. Кожен блок має фіксований час створення (для Біткоїна складає 10 хвилин). [2, с. 163]

## 1.4 Особливості технології блокчейн

Головною особливістю технології блокчейн є децентралізованість. Завдяки цьому досягається висока надійність всієї мережі: втрата декількох нод не спричиняє втрати всієї інформації. Розподіленість системи та відсутність посередників робить блокчейн ідеальним рішенням для мереж, між учасниками якої немає довіри. Правильність функціонування всієї системи забезпечується математичними алгоритмами. Принципи їх роботи визначені наперед і не можуть бути змінені жодною людиною, в тому числі творцем мережі.

До особливостей технології блокчейн можна також віднести прозорість. Кожен член мережі може завантажувати та переглядати повний ланцюжок блоків. Це сприяє утворенню довіри до системи. При збережені інформації використовується криптографічне шифрування.

# 2. Поняття та види консенсусу

Однією з основних технологій, які забезпечують децентралізацію і надійність криптовалют, є консенсус. Консенсус – це математичний алгоритм, за допомогою якого створюються нові блоки та перевіряються транзакції. Консенсус є певним погодженням між майнером та системою про умови та розмір винагороди за його роботу.

Оскільки мережа не має центрального органу контролю, підтримання правильної роботи лежить на плечах математичних алгоритмів. Протоколи консенсусу гарантують, що мережа функціонує правильно і не допускає махінацій зі сторони користувачів.[3]

## 2.1 Proof-of-Work

Найбільш популярним видом консенсусу є Proof-of-Work (“доказ роботи”). За даного виду консенсусу комісійна винагорода начисляється залежно від затраченої “роботи”. Під словом «робота» розуміють обчислювальні потужності комп'ютера, які були витрачені на обрахування хеш-суми. Найбільшу винагороду отримує той, хто першим знайшов правильний результат складної функції (у випадку Bitcoin - функція, заснована на деревах Меркля). Решта учасників верифікують отриманий майнером результат. При цьому простежується асиметричність – результат набагато швидше перевірити, ніж знайти.

Такий вид консенсусу не передбачає довіри між учасниками мережі. Окрім того, для приєднання до блокчейн мережі не потрібно дозволу. Це забезпечує надійність та правильність обрахунків хеш-суми. Безпеці також сприяє і те, що потенційна атака на мережу потребує значних потужностей і, відповідно, грошей, що зазвичай робить крадіжку економічно невигідною.

Головним недоліком PoW є енергозатраність. Кожен майнер витрачає великі потужності для обрахунку, однак винагороду отримує лише перший з них. Таким чином, ймовірність того, що певний майнер отримає комісію прямо пропорційна обчислювальним потужностям його комп'ютера.

Однією із криптовалют, яка використовує PoW, є Bitcoin. [4, 5]

## 2.2 Proof-of-Stake

Велика енергозатраність Proof-of-Work призвела до появи Proof-of-Stake (“доказ долі”). Принциповою відмінністю даного алгоритму від PoW є те, що PoS не потребує складних обрахунків. Завдяки цьому досягається вища швидкість транзакцій, порівняно з PoW. Щоб убезпечити мережу, майнерів зобов'язують заставляти свої власні криптовалютні активи. Таким чином, вони самі стають зацікавлені в надійності системи. Як слідує з назви, більшу винагороду отримує майнер, який володіє більшою долею криптовалюти. Однак, на відміну від PoW, винагорода начисляється не за створення нового блоку, а за обробку транзакцій.

Менша енегрозатратність алгоритму PoS є як перевагою, так і недоліком. Через значно менше споживання обчислювальних ресурсів комп’ютера, потенційні атаки не вимагають великих інвестицій в устаткування, відповідно, стають потенційно дешевшими. Однією із таких загроз є атака “Nothing at stake” (“Нічого на кону”). При зазначеній атаці зловмисник створює форк і рівномірно розподіляє коїни між двома ланцюгами. У випадку викриття форку, зловмисник все одно отримує вигоду. Одним із вирішень цієї проблеми, є протокол Casper, розроблений Владом Замфіреску для криптовалюти Ethereum. Протокол Casper запобігає цьому, анулюючи долю майнера при спробі ініціювання “Nothing at stake”. Таким чином, майнеру є що втрачати і головний принцип даної атаки (безпека активів) зловмисника, не задовільняється. [7]

На відміну від більшості інших протоколів, майнер мережі PoS обов’язково має коїни цієї мережі. У зв’язку з чим, учасник стає зацікавленим у рості даної

криптовалюти. Завдяки цьому, такі проблеми як “атака 51” і “Трагедія спільних ресурсів” малоймовірні.

Окрім певних проблем з безпекою, притаманних усім криптовалютам, PoS має більш суттєвий недолік. Принцип роботи даного консенсусу передбачає, що людям вигідно накопичувати коїни цієї мережі. Це призводить до концентрації активів і в подальшому може призвести до централізації, що суперечить принципам блокчейна.

На сьогоднішній день криптовалюта Ethereum (ETH) у процесі переходу від PoW до PoS.[4, 6]

## 2.3 Delegated Proof-of-Stake

З метою подолання недоліків Proof-of-Stake у 2014 році було створено Delegated Proof-of-Stake (“розподілений доказ долі”). Ця різновидність PoS дозволяє обирати валідаторів шляхом голосування, що дозволяє пришвидшити створення блоків та обробку транзакцій шляхом зменшення кількість валідаторів.

Вибори валідаторів відбуваються через голосування, де кожен stakeholder (власник великої кількості коїнів) може віддати свій голос за будь-якого кандидата. Перемагає валідатор з найбільшою кількістю голосів. Механізм виборів дозволяє обирати валідаторів до тих пір, поки 50% стекхолдерів не підтвердять, що цієї кількості достатньо для децентралізації. Після створення блоку валідатором він розділяє винагороду з тими, хто голосував за нього.

Валідатор-делегат, у свою чергу, зацікавлений в якісній роботі. Чим краще він виконуватиме свої повноваження, тим вищою буде його репутація і тим більшою буде винагорода. Механізм репутації дозволяє мотивувати найбільш надійних валідаторів: стекхолдери ймовірніше проголосують за людину з високою репутацією, бо це збільшить їхні шанси отримати винагороду.

Якщо валідатор, з якигось причин не зміг обробити транзакцію або згенерувати блок, на його місце буде обрано нового. Навіть при нормальній роботі,

через певний фіксований час кожного валідатора буде усунено і почнуться нові вибори.

DPoS сприяє децентралізації та більш справедливому винагородженні майнерів.

Bitshares та Steem використовують DPoS.[4, 8, 9]

## 2.4 Proof-of-Capacity

Proof-of-Capacity (“доказ ємності”) або Proof-of-Space – вид консенсусу, при якому ймовірність отримання комісійної винагороди корелюється з об’ємом дискового місця, наданого майнером. Даний вид майнінгу є більш енергоефективним та не потребує настільки великих затрат на комп’ютерні комплектуючі як PoW.

На перший погляд, PoC нагадує PoW, однак у них різний принцип роботи. Замість того, щоб обчислювати хеш-суму, її можливі результати (nonce) записуються на диски всіх майнерів у мережі. Чим більший дисковий простір надає майнер, тим більшу кількість рішень буде записано. Далі обирається правильний результат.

Механізм PoC складається з 2 кроків: заповнення та безпосередньо майнінгу. На першому етапі сховище майнера заповнюється нонсами, які вираховуються методом циклічного хешування певних даних. Кожен нонс складається з 8192 хешів (пронумерованих від 0 до 8191). Хеші попарно з’єднані і утворюють так звані scoops (пари). На другому етапі відбувається майнінг. Він полягає у прорахуванні номера пари. Після того, як майнеру стає відомий номер пари, він може прорахувати значення дедлайну (кінцевого терміну) за допомогою скоупа, що має номер, який було знайдено раніше. Мета майнера - знайти найменше значення дедлайну, щоб мати право створити новий блок і отримати винагороду.

PoC наразі не є популярним. Однієї із причин є його вразливість до вірусів - на інфікованому комп’ютері нонси можуть бути “зіпсовані”.

Прикладом криптовалюти яка використовує PoC є Burstcoin. [4, 10, 11]

## 2.5 Proof of Space-Time

Proof of Space-Time (“доказ ємності і часу”) утворений комбінацією двох консенсусів Proof-of-Space і Proof-of-Time(“доказ часу”).

PoST підвищує безпеку системи та гарантує, що між створенням блоків пройшов певний час. [12] Ключовою відмінністю від PoS є те, що PoST враховує час, протягом якого дисковий простір, відведений під запис нонсів, був незмінними. Протокол PoST вимірює “роботу” майнера в одиницях spacetime – об’єм дискового простору зарезервованого на певний час. [13]

Процес верифікації PoST довший порівняно з PoS.

Протокол став популярним завдяки криптовалюті Chia. Відомість автора валюти – Брема Коєна, творця протокола BitTorrent – забезпечила високу ліквідність криптовалюти ще на старті торгів.

Дефіцит відеокарт у 2020-2021 рр., який було викликано взлетом популярності Bitcoin, спричинив активний пошук альтернативних механізмів майнінгу. [14] Однак, розповсюдження криптовалюти Chia також призвело до дефіциту. На цей раз, під удар потрапити жорсткі диски (HDD) та твердотілі накопичувачі (SSD). [15]

## 2.6 Proof-of-Activity

Proof-of-Activity (“доказ активності”) є об’єднанням PoW і PoS, що дозволяє майнерам обирати яким чином вони хочуть отримувати комісію - через енергозатратні обрахунки чи закладання своєї долі. Метою PoA є поєднання переваг обох консенсусів і підвищення безпеки всієї системи.

Утворення нового блоку починається з обрахунку складної функції (риса PoW). Верифікацією новоутвореного блоку займаються обрані системою

валідатори. Люди, з більшою кількість коїнів даної мережі, мають більше шансів бути обраними валідаторами (риса PoS).

Proof-of-Activity перейняла від PoW і PoS разом з перевагами і недоліки. Попри те, що затрати електроенергії у PoA менші, ніж у PoW, вони все ще ж вищі за PoS. Також алгоритм PoA не надає дієвої протидії накопиченню та централізації активів.[4, 16]

# 3. Види криптовалют, їх задачі, характеристики, функції і властивості

“Криптовалюта – це цифрова або віртуальна валюта, яка захищена криптографією, що робить підробку майже неможливою”. [17] Переважна більшість криптовалют децентралізовані та використовують мережу блокчейн для свого функціонування.

## 3.1 Види криптовалют

### 3.1.1 Біткоїни та альткоїни

Існує декілька класифікацій криптовалют. За першою з них, усі криптовалюти на ринку можна розділити на біткоїни та альткоїни.

Біткоїн (BTC) створений 3 січня 2009 року, став першою криптовалютою. Попри те, що технічні характеристики Біткоїна на сьогоднішній день вже є застарілими, він досі залишається найбільш популярним серед криптовалют. Надійність та прозорість, на ряду з тривалим часом існування, дозволили BTC стати “електронним золотом”. [18]

Популярність Біткоїна призвела до виникнення низки нових криптовалют. Їх почали називати альткоїнами (альтернативні коїни). У технічному плані, більшість альткоїнів є форками Біткоїна. [19]

Головна мета альткоїнів - подолати недоліки BTC. Серед них можна виділити:

- низька енергоефективність;
- повільні транзакції;
- недостатня анонімність.

На початку свого існування проблема складних обчислень хеш-функції Біткоїна не стояла так гостро, оскільки алгоритм враховував сумарну обчислювальну потужність мережі: чим більшими потужностями по відношенню до сумарних володіє майнер, тим більша ймовірність отримання винагороди. Відповідно, із ростом числа нод, збільшується складність обчислення і зменшується прибутковість майнінгу. [20] За даними веб-ресурсу bitcoinity, складність майнінгу зросла у 14 разів, порівняно з початком існування Біткоїну.

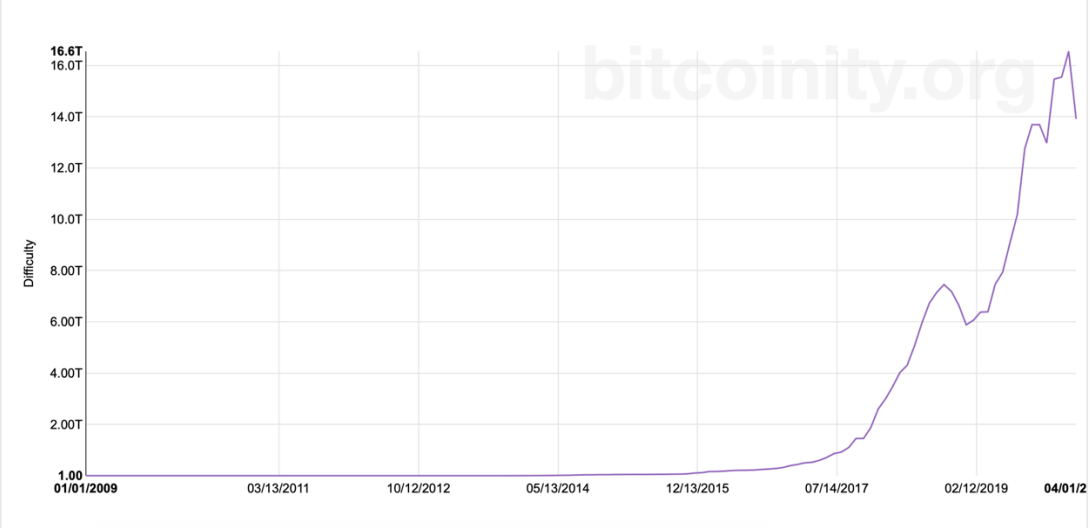


*Рис. 3.1.1.1 Ріст складності майнінгу Біткоїна з часом[21]*

Нові алгоритми консенсусу дозволяють зменшити вимоги до апаратної складової та підвищити енергоефективність, за рахунок альтернативних підходів до формування нових блоків та обробки транзакцій (використання дискового простору, застава власних коїнів).

Не варто забувати, що криптовалюти існують не лише для майнінгу, а і для розрахунків. Кінцевому користувачу дуже важливо мати можливість здійснювати швидкі перекази з низькою комісією. У випадку Біткоїна, комісія та швидкість обробки залежать від розміру транзакції: чим вона більша, тим менша комісія і швидша обробка. Для маленьких переказів час між відправленням і зарахуванням може сягати двох годин. Одним із підходів для пришвидшення обробки транзакцій

є зменшення розміру блока (Біткоїн кеш або BCH). Інші альткоїни досягають цього за рахунок спрощеного механізму валідації транзакцій або зменшення кількості валідаторів.

Для реєстрації рахунку, мережа Біткоїн не запрошує жодних персональних даних, однак вся інформація про транзакції зберігається у відкритому доступі на комп'ютерах майнерів. Правоохоронні органи, за потреби, можуть відстежити повний ланцюжок переказів і встановити особистість власника рахунку. Перша повністю анонімна криптовалюта ZCash (ZEC) надає механізм верифікації транзакцій без надання інформації про відправника, отримувача і суми переказу.[22] Інша популярна конфіденційна криптовалюта – Monero (XMR) - захищає дані своїх користувачів за допомогою протоколу CryptoNote, заснованого на механізмі кільцевих підписів. Кільцевий підпис є різновидом електронного підпису, який дозволяє підтверджувати конфіденційну інформацію без розкриття особистих даних, але гарантуючи її достовірність.[23] Варто також зазначити, що ряд сервісів для обміну криптовалют відмовляються працювати з анонімними цифровими валютами, через острах, що їх використовують для фінансування нелегальної діяльності.[24]

### 3.1.2 Класифікація за рівнем волатильності

Іншим способом класифікації є розділення криптовалют за рівнем волатильності. Волатильність – це коливання ціни протягом певного періоду часу. Виділяють звичайні та стейблкоїни (stablecoin).

На відміну від решти криптовалют, стейблкоїни прив'язані до фіатних грошей або іншого ліквідного активу (золота, нафти, діамантів тощо). Завдяки цьому, волатильність відсутня. Курс стейблкоїна прив'язується до курсу активу, яким він забезпечується.

Стейблкоїни поділяють на фіатно-забезпечені (fiat-collateralized), крипто-забезпечені (crypto-collateralized) та алгоритмічні. Для фіатно-забезпечених

стейблкоїнів характерна прив’язка 1:1 до фіатної валюти, якою вони забезпечуються. Центральний емітент зобов’язується зберігати суму фіатних грошей, пропорційну випущеним коїнам та надавати інструменти їхнього взаємного обміну. Для купівлі фіатно-забезпечених коїнів необхідно перевести таку ж суму у фіатній валюті на рахунок емітента. Якщо власник рахунку бажає повернути стейблкоїни, йому буде повернуто відповідну суму у фіатній валюті, а “повернені” стейблкоїни будуть знищені. Головною проблемою фіатно-забезпечених валют є централізованість і наявність емітента, якого необхідно перевіряти на доброчесність.

Крипто-забезпечені стейблкоїни використовують криптовалюту у якості завдатку. Криптовалюта нематеріальна, тому випуск забезпечується смарт-контрактами. Даний вид стейблкоїна дозволяє прибрати емітента, а отже і проблеми пов’язані з ним. При купівлі крипто-забезпечених коїнів, еквівалентна сума іншої криптовалюти блокується за допомогою смарт-контракту. Для повернення застави необхідно переказати свої стейблкоїни на цей же контракт.

На відміну від двох попередніх видів, алгоритмічні стейблкоїни забезпечують низькі коливання курсу, за допомогою алгоритмів. Алгоритми відслідковують курс певної валюти, до якої прив’язаний стейблкоїн. Залежно від зміни курсу приймається рішення, щодо об’єму випуску коїнів. При підвищенні курсу коїна відносно фіатної валюти - випуск збільшується, при понижені курсу - зменшується.[25]

Найпопулярнішим стейблкоїном є фіатно-забезпечений Tether (USDT), який прив’язаний до долара у відношенні 1 до 1. Станом на 2020 рік, він входить в п’ятірку найбільших криптовалют за рівнем капіталізації, на рівні з Bitcoin та Ethereum. Tether було створено у 2014 році. Він став першим стейблкоїном у світі.

USDT випускається на різних блокчейнах: Bitcoin (через Omni Layer), Ethereum, TRON, EOS, Algorand, Solana. Найбільше коїнів було створено на платформі Ethereum, де Tether випускається у вигляді токена за протколом ERC-20.

Tether, на ряду з іншими стейблкоїнами, використовується трейдерами для торгівлі звичайними криптовалютами, задля уникнення негативних наслідків волатильності. Тим самим, нівелюється розрив між фіатними та криптовалютами.[26]

### 3.1.3 Класифікація за видом блокчейн платформи

Криптовалюту можна також поділяти за видом платформи. Існує 3 види блокчейн платформ: публічні, приватні та гібридні. Публічні блокчейни надають кожному охочому можливість переглядати історію транзакцій та стати майнером. Наряду з підвищеною безпекою і децентралізованістю, це призводить до пониження продуктивності. У свою чергу, приватні можуть регулювати, хто має право переглядати список переказів та долучатись до мережі. Приватні платформи не забезпечують конфіденційності, тому найбільш ефективним є використання наперед визначених валідаторів. При спробі протиправних дій, особистість зловмисника можна легко встановити. Гібридні блокчейни поєднують у собі риси обох платформ. Валідаторами можуть бути як закрите коло осіб, так і кожен бажаючий, залежно від вмісту блоку.[27]

## 3.2 Задачі криптовалют

До задач криптовалют відносять:

- безпеку;
- проведення конфіденційних платежів;
- розрахунки без посередників;
- цифровізація активів або токенізація.

Незважаючи на низький рівень довіри, криптовалюти є безпечними. Завдяки збереженню історії транзакцій децентралізовано підвищується надійність. Втрата

однієї ноди не призводить до втрати інформації. Це також ускладнює підробку даних зловмисниками. Кожна транзакція верифікується певною кількістю майнерів, а сам принцип технології блокчейн унеможливлює підробку старих записів.

Наступною задачею є проведення конфіденційних платежів. Розподілений реєстр криптовалюти не містить жодних персональних даних: ні транзакції, ні облікові записи не пов'язані з будь-якою особистою інформацією користувача. Дані про переказ складаються з: часу, суму, публічних ключів відправника та отримувача. [28] Однак, не варто забувати, що вся інформація про транзакції міститься у відкритому доступі, і може бути використана для відслідковування повного ланцюжка переказів і встановлення ідентичності його власника. Якщо існує потреба у повністю анонімному платежі, на ринку існують рішення, такі як ZCash та Monero.

Як було зазначено в попередніх розділах, мережа блокчейн позбавлена посередників – функціонування забезпечують самі учасники системи. Таким чином, можна позбавитись одразу від двох проблем: ніхто не може зупинити/затримати транзакцію та немає потреби перевіряти посередника на доброчесність. Мережа блокчейн не слідкує за тим куди і скільки ви переказуєте коїнів, на відміну від банківських переказів, які потребують часу для перевірки і можуть бути відміненими, якщо у служби безпеки виникли сумніви. Навіть безготівковий розрахунок фіатними грошима потребує участі банку. Відсутність посередників також дозволяє зменшити комісію. Це робить криптовалюту ідеальним рішенням для клірингу (міжнародних безготівкових переказів).

Токенізація – це цифрове представлення певного існуючого активу у децентралізованому реєстрі. У процесі цифровізації активів випускаються токени.[29, 30]

Під терміном токен розуміють вид цифрової валюти, яка є одиницею вартості. Однак, токени використовуються в задачах, для яких не підходять криптовалюти.

Розглянемо токени на прикладі найпопулярнішого протоколу ERC-20 (Ethereum Request for Comments). Цей прокол було розроблено платформою Ethereum для вирішення проблеми сумісності різних форм токенів. Протокол ERC-20 дозволяє зробити всі токени взаємозамінними і економить час для створення власної блокчейн мережі – натомість використовується існуюча інфраструктура Ethereum. Токени зберігаються в контрактах, у яких зазначаються їх характеристики (назва, символ тощо). Також контракти містять поточні баланси усіх користувачів. Особливістю є те, що власнику токенів потрібно мати криптовалюту Ethereum на своєму гаманці для проведення переказів. З точки зору платформи, перекази токенів є звичайною транзакцією. Тому за кожен переказ необхідно сплатити комісію.

Головною відмінністю токенів від криптовалюти є те, що емісія токенів не завжди проводиться децентралізовано. Те саме стосується і верифікації транзакцій. Також токени неможливо “майнити”. Ціна токенів регулюється не лише співвідношенням попиту і пропозиції – є можливість прив’язати власний токен до курсу іншого. Як було зазначено вище, токени необов’язково запускаються на власній блокчейн мережі. [31, 32]

## 3.3 Характеристики криптовалют

Ключовою характеристикою криптовалют є використання технології блокчейн. Саме це обумовлює дві наступні риси - розподіленість і захист від модифікацій. Зберігання бази даних усіх переказів у відкритому доступі на комп’ютерах учасників мережі дозволяє гарантувати прозорість системи.

Об’єм випуску і правила обігу криптовалют підпорядковується математичному алгоритму і не можуть бути змінені централізовано. Для більшості криптовалют характерним є волатильність, оскільки курс коїна залежить лише від попиту і не може бути урегульований ззовні грошовою політикою.

Ще однією характеристикою криптовалюти – відсутність автентифікації. Попри те, що інформація про всі транзакції зберігається у відкритому доступі, особисті дані власника гаманця не відомі навіть самій мережі. Доступ до рахунку має кожен, кому відома пара публічного і приватного ключа.

Наступною характеристикою криптовалют є швидкість виконання транзакцій. Завдяки тому, що система не має посередників і регіональної прив'язки, швидкість обробки переказу залежить лише від платформи і суми. Усунення "людського фактору" дозволяє гарантувати стабільну швидкість навіть у вихідні та святкові дні. З часу запуску Біткоїну у 2009 році, мережа функціонувала 99.98% часу. Одна з найшвидших криптовалют Ripple здатна обробити до 50 тисяч транзакцій за секунду. Для порівняння, Visa має пропускну здатність лише 24 тисячі транзакцій за секунду.[33]

Криптовалюти з обмеженою емісією мають ще одну характеристику – "природну" дефляцію. Дефляція – це загальне зниження вартості товарів і послуг, при від'ємному рівні інфляції. Таким чином, піднімається вартість самої валюти. Це також може свідчити про ріст купівельної спроможності населення. Завдяки тому, що об'єм випуску криптовалют є обмеженим, в якийсь момент на ринку буде дефіцит коїнів. Наприклад, емісія Біткоїна обмежена 21 мільйоном одиниць, але з часом коїнів буде ставати все менше: люди втрачатимуть приватні ключі і криптовалюта на їхніх рахунках ставатиме недоступною. [34]

## 3.4 Функції криптовалют

Криптовалюти виконують усі функції фіатних грошей.

До функцій грошей відносять:

- еквівалент вартості;
- розрахунки;
- платежі;
- накопичення;

- світові гроші.

Еквівалент вартості дозволяє порівнювати, обмінювати та встановлювати ціни на матеріальні товари та послуги. Для цієї функції важлива стабільність ціни валюти, щоб уникнути ризику коливання ціни під час транзакції. Криптовалюти поки що незручно використовувати для даної функції, через високу волатильність(окрім стейблкоїнів). [35, 36]

Наступною функцією є засіб розрахунку. Під поняттям розрахунок криптовалютою мають на увазі, можливість її переказу та отримання на публічний ключ. Для ефективного виконання даної функції важлива ліквідність активу (здатність до швидкого і легкого продажу по ціні наближеній до ринкової) та швидкість операцій. Популярні криптовалюти мають високу ліквідність. На відміну від фіатних грошей, швидкість транзакцій криптовалют не є сталою та залежить від платформи. Так, швидкість розрахунку Bitcoin становить до 60 хвилин, в той час як Ripple та Stellar дозволяють проводити транзакції на швидкості 4 секунди.[37]

Криптовалюту частково можуть використовувати як платіжний засіб. Станом на 2018 рік, 8 країн повність заборонили використання та проведення розрахунків криптовалютою.[38]

Ще однією важливою функцією будь-якої валюти є накопичення та збереження вартості. Обмежена емісія і портативність криптовалюти роблять їх хорошим засобом накопичення, попри високу волатильність. Деякі види консенсусу (наприклад Proof-of-Stake) напряму заохочують до накопичення коїнів.[39]

Криптовалюти ідеально підходять у якості світових грошей, бо, на відміну від фіатної валюти, не мають прив’язки до жодної країни.

Найкраще функції грошей виконує Bitcoin, оскільки має найбільшу ліквідність та капіталізацію.

## 3.5 Властивості криптовалют

Гроші мають наступні властивості:

- непідробність;
- рідкість;
- однорідність;
- ділимість та об’єднуваність;
- зберігаємість;
- портативність;
- вартісна стабільність;
- загальне визнання.

Тепер детальніше розглянемо, яким чином криптовалюта задовольняє вищеописані властивості. Децентралізований характер криптовалют робить потенційну спробу підробки технічно неможливою. Новітні протоколи (наприклад, раніше згаданий протокол Casper) можуть анулювати кошти користувача за спробу ініціювання протиправних дій. Безпека і непідробність також забезпечується завдяки громіздким обчисленням (PoW) або особистій зацікавленості учасників мережі (PoS).

Завдяки тому, що криптовалюти мають обмежену емісію, вони задовольняють властивість рідкості.

Однорідність гарантує, що кожна одиниця грошової маси має однакову якість і вартість. Це досягається завдяки тому, що кожен коїн криптовалюти створюється, зберігається і ходить в обігу за однаковими правилами.

Для грошей також є властивим здатність до поділу, при тому сукупна вартість утвореної маси повинна збігатись з початковою. Криптовалюти можна розділяти та об’єднувати. Мінімальна частина Біткоїна - 1 сатоши, що становить одну стомільйонну частину BTC.

Термін зберігаємість означає, що цінність грошей буде незмінною протягом значного проміжку часу. Це є необхідним для забезпечення багаторазового

використання валюти. Криптовалюти не мають фізичного представлення і зберігаються розподіллено у базі даних. Таким чином, у вони задовольняють дану властивість краще за фіатні валюти.

Ще однією властивістю з якою цифрові гроші справляються краще ніж фіатні, є портативність. Доступ до криптовалюти можна отримати цілодобово, за умови наявності інтернет підключення. Для цього достатньо знати публічний і приватний ключ власного рахунку.

Наступна властивість грошей - відсутність значних коливань у вартості, або вартісна стабільність. Лише деяким криптовалюти притаманна дана властивість – стейблкоїни. Обмеженість грошої маси, яка поступає в обіг, гарантує, що вартість залишатиметься на відносно однаковому рівні.

Останньою властивістю є загальне визнання. Це єдина властивість, якої ще не набули криптовалюти. Наразі, лише деякі країни надають можливість розрахунків криптовалютою на рівні з фіатними грошима. Найбільш визнаним і, відповідно, ліквідним є Bitcoin, який заслужив статус “електронного золота”.[40, 41]

# 4. Порівняння криптовалют з фіатними грошима

“Фіатна валюта – це узаконений платіжний засіб, цінність якого встановлюється урядом і випускається ним”. Оскільки фіатні валюти не забезпечуються золотом чи іншим ліквідним фізичним товаром, цінність валюти залежить від міжнародного авторитету держави та довіри населення. Фіатні валюти не мають внутрішньої цінності – країні практично нічого не коштує випустити нову одиницю, оскільки її не треба забезпечувати. Неправильна політика випуску фіатних грошей може стати причиною інфляції. [42]

Перш за все, відмінність криптовалюти та фіатних грошей лежить у способі збереження інформації про перекази та власників рахунків. Записи про транзакції криптовалют зберігаються у розподіленій базі даних за допомогою технології блокчейн. У той час як для фіатних валют характерне консолідоване збереження. Це робить національні валюти більш вразливими до атак і технічних проблем – втрата даних у Центральному банку призведе до втрати всіх даних.

Уся робота мережі блокчейн підпорядкована математичним алгоритмам, які відомі наперед і не можуть бути змінені централізовано, навіть творцем. Таким чином, емісія і об’єм випуску криптовалюти є незмінними і відомими заздалегідь(окрім стейблкоїнів). Політика випуску і обігу фіатних валют підпорядковується Центральному банку або іншим державним інститутам.

Як і криптовалюти, фіатні гроші не забезпечуються жодним фізичним товаром або продуктом і не мають внутрішньої цінності. Винятком є стейблкоїни які можуть забезпечуватись як ліквідним фізичним активом так і іншою криптовалютою.

У той час як курс фіатних валют регулюється політикою Центрального банку, для криптовалют характерною є волатильність. Як було зазначено вище, принципи емісії криптовалют є незмінними, тому курс залежить від співвідношення попиту і пропозиції. Таким чином, на ціну впливає великий перелік факторів: економічна

ситуація у світі, новини, зміни в законодавстві, оновлення платформи криптовалюти тощо. Після того як Ілон Маск додав хештег #bitcoin в описі власної сторінки у соціальній мережі Twitter, вартість Bitcoin підвищилась на 19%. [43] На графіку нижче продемонстровано зміну індексу волатильності Bitcoin відносно USD.

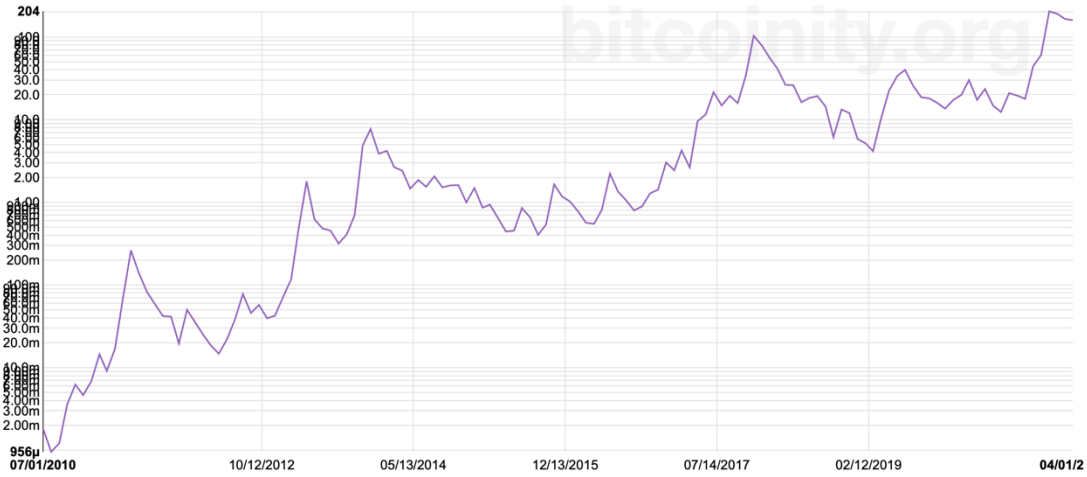


*Рис. 4.1 Індекс волатильності Bitcoin відносно USD[44]*

Криптовалюти не мають фізичного носія, що теж відрізняє їх від фіатних валют.

Наступною відмінністю є конфіденційність. У мережі блокчейн не зберігається жодних персональних даних користувача. Щоб зареєструвати гаманець не потрібно вводити ні паспортні дані, ні код платника податків. Для доступу до особистого рахунку використовується пара публічного і приватного ключа. Таким чином, при втраті цих даних, відновити доступ до гаманця буде неможливо. На противагу, фіатні валюти можуть зберігатись готівкою або на рахунку банку. Якщо розрахунки готівкою є анонімними, то для реєстрації банківської карти потрібно вносити персональні дані до системи. Тому при втраті карти, доступ до неї можливо відновити.

Якщо фіатні валюти можуть вводити в обіг лише держави, то криптовалюти має можливість створити будь-яка особа. Тому цифрові валюти також носять умовну назву “приватні гроші”.

З цього випливає ще одна відмінність. Криптовалюти не є загально визнаними, як було сказано в попередньому розділі, і їхнє використання у якості грошей не є обов'язковим та обумовлюється лише бажанням людей. У той час як, фіатні валюти є обов'язковими для прийому у якості плати за усі товари і послуги на території держави емітента.

Фіатні валюти регулюються державою, на відміну від криптовалюти.

Транзакцію криптовалютою неможливо відмінити. Єдиний спосіб повернути коїни, якщо вони, наприклад, були перераховані на неправильний рахунок, це попросити власника іншого гаманця відправити їх назад. Зрозуміло, що даний метод не є ефективним.

Фіатні гроші за своєю природою є інфляційними, у той час як криптовалюти – дефляційними. Причиною є об'єм грошей. Дефіцит грошової маси, викликаний обмеженою емісією, спричиняє дефляцію. Відповідно її профіцит – інфляцію.[45]

# 6. Практична частина

## 6.1 Створення криптовалюти

### 6.1.1 Теоретичне підґрунтя для створення криптовалют

Криптовалюти можна поділити на два види: коїни та токени. Головною їхньою відмінністю є те, що коїни функціонують на власній блокчейн мережі, у той час як токени можна створювати на існуючих платформах (Ethereum, NEO, Ripple, EOS). З огляду на це, при використанні токенів можна суттєво зекономити час для розгортання власної мережі та використовувати платформи, які вже зарекомендували себе з точки зору безпеки та зручності.

Варто зауважити, що між токенами і коїнами існує важлива відмінність – токени неможливо майнити.

Токени містяться в контрактах, які визначають їхні характеристики та реалізують необхідні методи для роботи з криптовалютою. У контракті зберігаються баланси усіх користувачів.

Оскільки токени розгортаються поверх існуючої інфраструктури, то вони переймають деякі її властивості. Тому вибір платформи є важливим етапом у розробці криптовалюти. Наприклад, токен, створений на Ethereum, буде мати швидкість 15 транзакцій за секунду та базуватись на консенсусі Proof-of-Work.

Від платформи залежить мова програмування, а не тільки кінцеві якості токену. Розробка криптовалюти на платформі Ethereum ведеться мовою Solidity (власна мова Ethereum), при тому як NEO та EOS дозволяють використовувати більшість високорівневих мов, таких як C++ та Python. [46]

У нашій роботі описано створення токену на платформі Ethereum. Оскільки, створення криптовалюти є платним, було прийнято рішення розгортати власну криптовалюту у тестовій мережі.

### 6.1.2 Особливості створення токену на мові Solidity

#### 6.1.2.1 Стандарт ERC-20

У даній роботі розглянуто створення токену за стандартом ERC-20 з визначеними додатковими методами для продажу/купівлі токенів. (такі токени мають назву Mintable).

Для створення токену за стандартом ERC-20 необхідно реалізувати визначений перелік методів:

- totalSupply() – кількість випущених токенів;
- balanceOf(param) – повертає кількість токенів, які містяться на рахунку, у якості параметра приймає адресу;
- transfer(address, value) – результатом методу є переміщення певної кількості токенів (value) на рахунок address;
- transferFrom(address1, address2, value) результатом методу є переміщення певної кількості токенів (value) з рахунку address1 на рахунок address2;
- approve(address, value) – встановлює кількість власних коїнів(value), яку власник рахунку дозволяє витратити іншому користувачу(address);
- allowance(address1, address2) – специфічний метод для стандарту ERC-20 – повертає кількість невитрачених коїнів, яку власник рахунку address2 може витратити від імені власника рахунку address1.

За потреби, можна додатково визначити декілька властивостей:

- name() – назва нашого токену;
- symbol() – позначення для токену;
- decimals() – кількість знаків після коми, визначає на скільки частин може бути розбитий токен(наприклад долар(USD) мав би значення 2). [31]

#### 6.1.2.2 Особливості обчислення в Solidity

Особливістю мови Solidity є те, що у ній не використовується тип float. Таким чином, 1 коїн зі значенням decimals 2 буде зберігатись як цілочисельний тип зі значенням 100. [47]

Через використання великих чисел, існує ймовірність переповнення і, відповідно, некоректної роботи токену. Тому загальноприйнятим стандартом є використання бібліотеки SafeMath.

```
contract SafeMath {
    function safeAdd(uint a, uint b) public pure returns (uint c) {
        c = a + b;
        require(c >= a);
    }
    function safeSub(uint a, uint b) public pure returns (uint c) {
        require(b <= a);
        c = a - b;
    }
}
```

*Рис. 6.1.2.2.1 Приклад використання SafeMath.*

### 6.1.3 Обґрунтування вибору засобів та інструментів розробки

У якості середовища для створення та розгортання токену використовується Ethereum Wallet та Remix. Спочатку розробка велась у програмі Ethereum Wallet, оскільки це застосунок розроблений самою платформою Ethereum. Однак, при роботі було помічено багато критичних помилок (деякі версії програми не запускаються, при переході на власну мережу інтерфейс “з’їжджає”). Тому було прийнято рішення шукати альтернативи.

Найпопулярнішим рішенням для розробки токенів є Remix – Ethereum IDE з відкритим вихідним кодом. Серед переваг можна навести наявність версії для браузера.

Для роботи в Remix також необхідно завантажити MetaMask – розширення для браузеру (доступний для Chrome, Firefox, Brave та Edge). MetaMask надає не лише функціонал криптовалютного гаманця, а й дозволяє під’єднатись до децентралізованих застосунків (DApps) та сайтів, що містять інтеграцію з Ethereum.

MetaMask дозволяє перемикатись між основною та тестовими мережами. Для даної роботи було використано тестову мережу Popsten, оскільки вона є найбільш популярною.

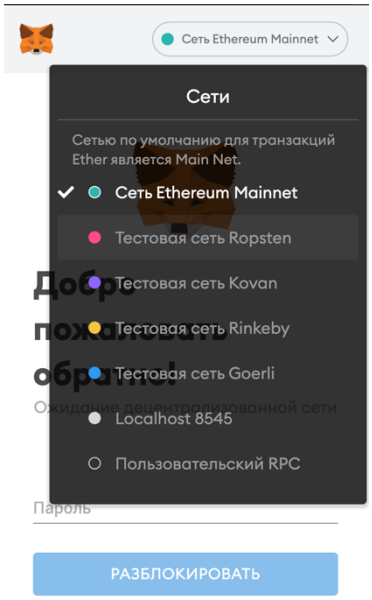


*Рис. 6.1.3.1 Перемикання між мережами в розширенні MetaMask.*

### 6.1.4 Створення та розгортання токену

Для запуску токену необхідно перемістити код в IDE та перейти на вкладку “Solidity Compiler”, обрати мову (у нашому випадку Solidity) та скомпілювати.

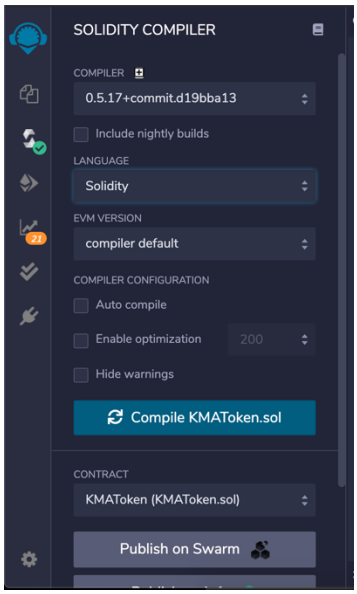


*Рис. 6.1.4.1 Компіляція контракту у застосунку Remix.*

Після успішного виконання попереднього кроку, переходимо на вкладку “Deploy and run transactions”. Далі обираємо потрібні параметри Environment та Gas Limit. Для нашої роботи було обрано Injected Web3 та 3 млн. Також обираємо гаманець (Account), який потрібний для оплати розгортання контракту. Оскільки, запуск ведеться в тестовій мережі, то оплатити можна фальшивою (fauset) криптовалютою (отримати фальшиві ETH можна за допомогою сайту https://faucet.ropsten.be).

Після цього нам буде запропоновано оплатити комісію та підтвердити розгортання контракту.

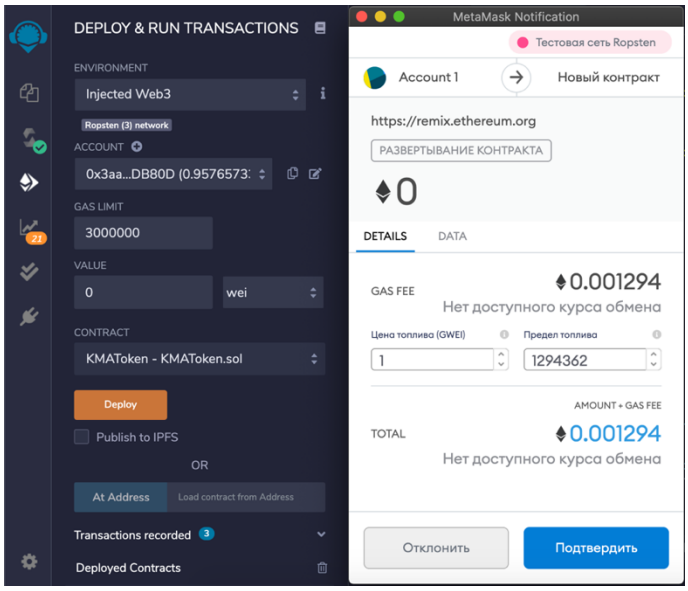


*Рис. 6.1.4.2 Розгортання контракту у застосунку Remix.*

При успішному створенні токену, з’явиться запис про розгортання контракту у вкладці “Активність” у MetaMask.

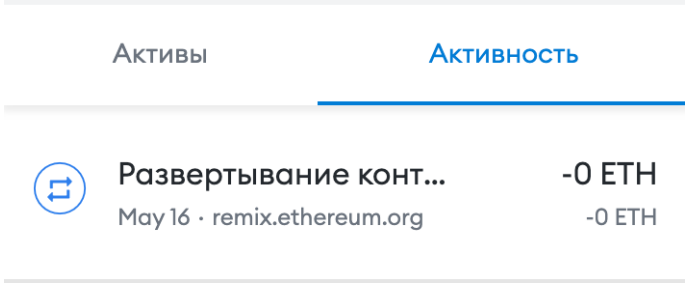


*Рис. 6.1.4.3 Підтвердження розгортання у розширені MetaMask.*

## 6.2 Створення застосунку для зберігання і купівлі NFT токенів

### 6.2.1 Опис застосунку

Нашою задачею було розробити застосунок для зберігання та купівлі NFT токенів, під’єднаний до Ethereum гаманця MetaMask. У якості предметної області було обрано цитати. Крилаті вислови гарно ілюструють суть NFT токенів: вони мають бути унікальними, належати лише одній людині та мати різну значимість (деякі афоризми зберігаються крізь віки, інші – забуваються через рік).

Інтерфейс програми складається з даних про акаунт (адреса та баланс) та списку цитат користувача.

При початковому розгортанні застосунку список афоризмів пустий.

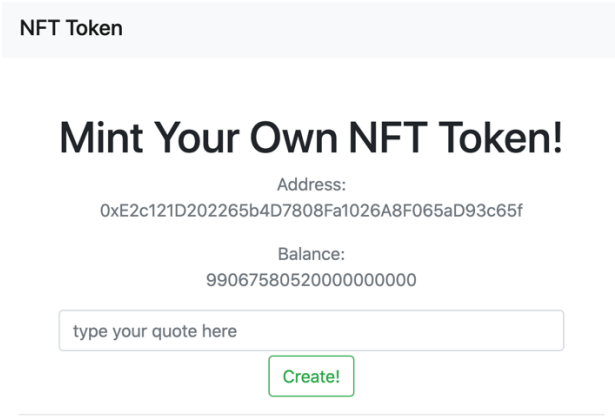


*Рис. 6.2.1.1 – Інтерфейс програми.*

Для того, щоб додати цитату, потрібно ввести її в поле та натиснути кнопку “Create!”. Після цього користувачу буде запропоновано оплатити токен за допомогою MetaMask.

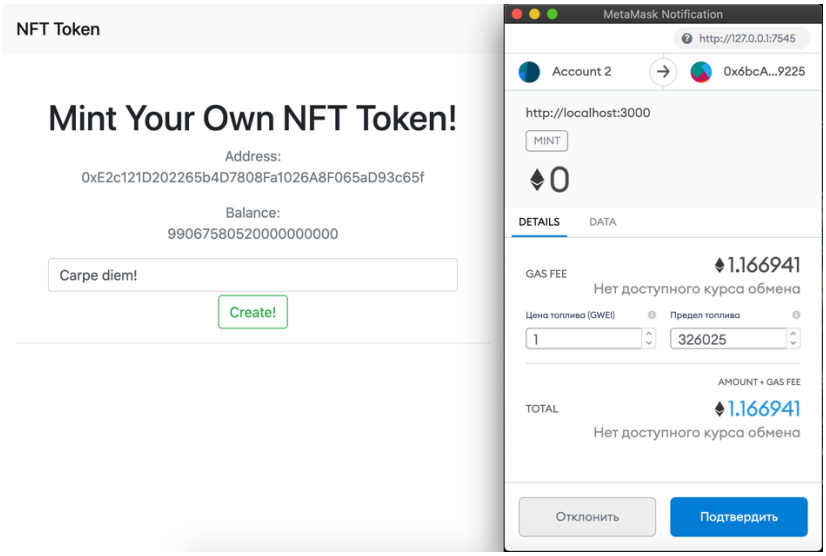


*Рис. 6.2.1.2 Підтвердження створення токену.*

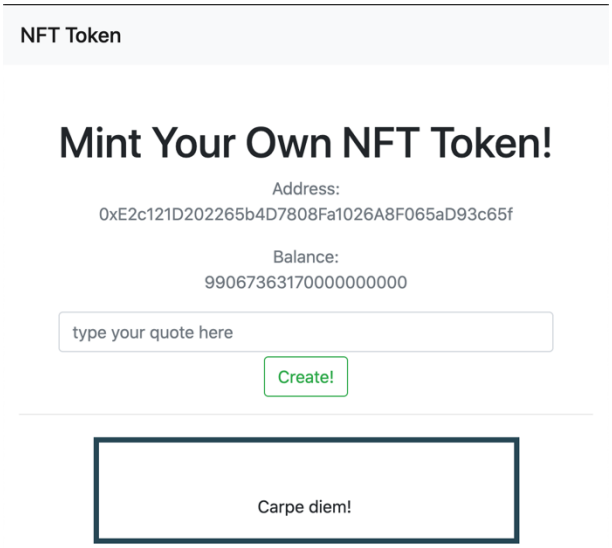


*Рис. 6.2.1.3 Утворений токен додано до колекції користувача.*

### 6.2.2 Теоретичне підґрунтя

“Не взаємозамінні токени (NFT) – це тип криптографічного токену, який представляє собою унікальний актив. NFT – це токенізована версія цифрових або реальних активів”. [48] Як слідує з назви, NFT токени не рівнозначні та унікальні.

На відміну від решти криптовалют і фіатних грошей, які гарно підходять як засіб розрахунку через свою однорідність, NFT використовуються для продажу та купівлі цифрових колекційних предметів. Оскільки, кожен NFT токен

розглядається як окрема унікальна одиниця, є можливість встановлювати різну вартість для різних активів.

NFT токени широко використовуються у сфері цифрового мистецтва зважаючи на те, що технологія гарантує унікальність та непідробність роботи, унеможливлюючи її копіювання.

Аналогічно до звичайних токенів, для NFT було розроблено низку стандартів. При розробці було використано найпопулярніший протокол ERC-721. [48]

### 6.2.3 Обґрунтування вибору засобів та інструментів розробки

Для розробки серверної частини було використано Node.js, яка є найбільш затребувана платформа на сьогоднішній день. [49] Вона надає потужні інструменти для роботи з асинхронністю, яка необхідна для взаємодії з контрактами.

Для графічного інтерфейсу обрано бібліотеку React та Bootstrap. Реактивна парадигма, використаний у React, дозволяє у відповідь на дії користувача миттєво оновлювати пов’язані значення. Bootstrap – це бібліотека для побудови користувацьких інтерфейсів, яка дозволяє легше створювати GUI, порівняно з використанням чистого CSS.

Використання JavaScript на серверній та клієнтській стороні дозволяє зробити архітектуру більш прозорою та гнучкою.

Для роботи з мережею блокчейн та смарт-контрактами використовується середовище Truffle, яке надає інструменти для компілювання, розгортання та тестування контрактів через CLI(Command Line Interface).

Окрім цього, для функціонування програми необхідно розгорнути тестову блокчейн мережу. Для цієї задачі було обрано Ganache – застосунок, який створює мережу на локальній машині. При його запуску, створюється 10 акаунтів, кожен з

яких містить 100 фальшивих ETH. Нам потрібен лише один, для сплати комісії за розгортання контракту.

Для підключення акаунту до застосунку використовується MetaMask. Для цього необхідно переключити MetaMask на локальну мережу та імпортувати гаманець з Ganache за допомогою закритого приватного ключа.

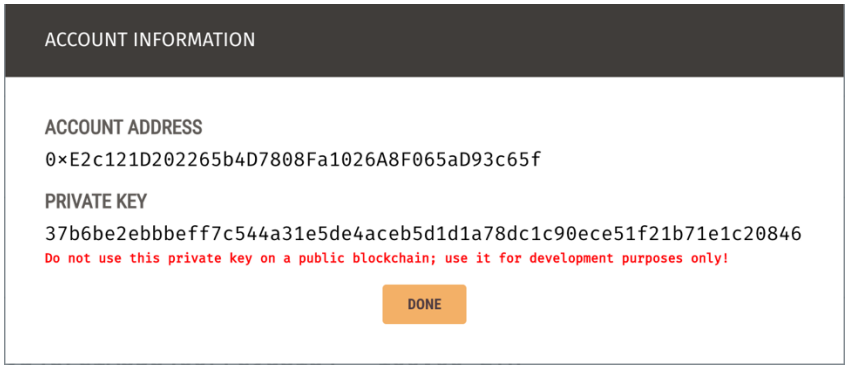


*Рис. 6.2.3.1 Приватний ключ від акаунту у застосунку Ganache.*

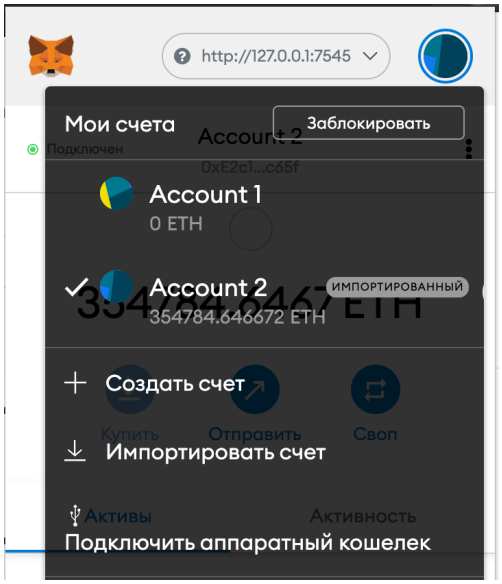


*Рис. 6.2.3.2 Імпортований гаманець у розширені MetaMask.*

Для прискорення розробки смарт-контрактів було додано бібліотеку OneZeppelin. Вона містить реалізацію більшості популярних протоколів (у тому числі необхідний нам ERC-721) та Solidity компоненти для розробки власних токенів.

### 6.2.4 Розробка застосунку

#### 6.2.4.1 Створення та запуск токена

Як зазначено вище, для розробки токену ми використовуємо OneZeppelin.

Наш токен буде наслідувати інтерфейс ERC721Full, який ми імпортуємо з бібліотеки, мати назву Quote і позначення QOT. Окрім того, у контракті зберігається список усіх цитат конкретного користувача та асоціативний масив, що ставить у відповідність кожній цитаті значення bool для відображення, які цитати вже комусь належать. При виклику метода mint ми перевіряємо, чи була дана цитата уже створена, за допомогою ownedQuotes, щоб гарантувати унікальність кожного токена.

```
pragma solidity 0.5.0;
import "@openzeppelin/contracts/token/ERC721/ERC721Full.sol";

contract Quote is ERC721Full {

    string[] public quotes;
    mapping(string => bool) ownedQuotes;

    constructor() ERC721Full("Quote", "QOT") public {...}

    function mint(string memory quote) public {
        require(!ownedQuotes[quote]);
        _mint(msg.sender, quotes.push(quote));
        ownedQuotes[quote] = true;
    }
}
```

*Рис. 6.2.4.1.1 Смарт-контракт написаний мовою Solidity.*

#### 6.2.4.2 Під’єднання до мережі Ethereum

Для під’єднання до мережі Ethereum, необхідно створити екзепляр web3. MetaMask використовує провайдер EIP-1193, який у бібліотеці Web3 доступний як window.ethereum. З урахуванням того, що нам потрібен MetaMask для нашого застосунку, перевіряємо чи браузер його підтримує.

```
async connectMetaMask() {
  if (window.ethereum) {
    window.web3 = new Web3(window.ethereum);
    await window.ethereum.enable();
  } else {
    alert("MetaMask is required to use this app");
  }
}
```

*Рис. 6.2.4.2.1 Під'єднання до мережі Ethereum.*

### 6.2.4.3 Взаємодія з акаунтами та контрактами

На сторінці застосунку відображається два блоки інформації: дані про акаунт та токени. Пакет web3.auth надає інструменти для доступу та перегляду усіх акаунтів в мережі. Метод getAccounts() повертає нам усі акаунти MetaMask під'єднані до сайту.

```
const web3 = window.web3
const accounts = await web3.eth.getAccounts()
const accountBalance = await web3.eth.getBalance(accounts[0]);
```

*Рис. 6.2.4.3.1 Доступ до даних акаунта.*

З урахуванням того, що наша програма не може функціонувати без NFT токену, перед подальшою роботою необхідно перевірити, чи контракт розгорнуто в мережі.

```
const net = await web3.eth.net.getId()
if (!Quote.networks[net]) {
  window.alert('Deployed contract is required to use this app')
}
```

*Рис. 6.2.4.3.2 Перевірка чи контракт розгорнуто в мережі.*

# Висновки

Після детального ознайомлення з технологією блокчейн та її особливостями, можна зробити висновок, що дана технологія є досить потужною та гнучкою, що дозволяє їй завойовувати все більшу популярність з кожним роком. Принципи, закладені в основу технології, дозволять їй ще довгий час залишатись актуальною та затребуваною. На момент написання курсової, технологія блокчейн знаходиться в своєму розквіті та набуває статусу нового стандарту збереження інформації. Розподілене зберігання даних дозволяє подолати низку проблем: від безпеки та прозорості до швидкості доступу.

Метою курсової було висвітлити технологію блокчейн та види консенсусів, які є невід'ємною її частиною та забезпечують правильне функціонування всієї системи. Наступним кроком було детально розглянути криптовалюти, які нерозривно пов'язані з технологією блокчейн. Саме використання блокчейну обумовлює певні переваги та недоліки криптовалют.

Консенсус є одним із китів, на яких тримається технологія блокчейн. Він забезпечує верифікацію записів та правильне утворення нових блоків. Найстарішим та найпопулярнішим видом є Proof-of-Work, використаний у Bitcoin. Однак, його низька швидкість та енергоефективність спричинили появу низки нових алгоритмів. Деякі криптовалюти, як Ethereum, відмовляються від застарілого Proof-of-Work в угоду новим. Ще одним популярним рішенням є Proof-of-Stake. Він є більш енергоефективним, але спонукає користувачів до накопичення коїнів мережі. Delegated-Proof-of-Stake є удосконаленням попереднього консенсусу. Він дозволяє обирати валідаторів, що призводить до пришвидшення верифікації транзакцій та більш справедливому розподіленню комісійної винагороди. DPoS було створено щоб подолати проблему концентрації, і відповідно, централізації криптовалюти. Proof-of-Capacity дозволяє майнити криптовалюту на пристроях без високої обчислювальної потужності, навіть смартфонах. Натомість

використовується дисковий простір. Не зважаючи на усі переваги, консенсус не став поширеним. Алгоритм Proof-of-Space-Time, розроблений на основі PoC, у 2021 році став неймовірно популярним, через нестачу відеокарт. Таким чином, неможливо виділити найкращий консенсус. Кожен із них пропонує власний спосіб вирішення проблеми швидкості та енергоефективності. Тому потрібно обирати, який вид консенсусу буде найоптимальніший для кожної задачі.

Існує безліч класифікацій криптовалют для упорядкування різноманіття коїнів. Перш за все, усі криптовалюти можна поділити на Bitcoin та альткоїни. Альткоїни виникли як відповідь на потребу людей у більш зручному та потужному інструменті. Деякі альткоїни покликані покращити енергоефективність, завдяки новітнім консенсусам. Інші роблять криптовалюту більш комфортною для кінцевого користувача, шляхом пришвидшення транзакцій. Це досягається також завдяки консенсусам, які зменшують час на верифікацію завдяки зменшенню числа валідаторів або розміру блока, використанню спрощеного механізму перевірки тощо. За останні 10 років, швидкість обробки переказів скоротилась з 2 годин до 4 секунд.

Стейблкоїни дозволяють позбавитись волатильності, притаманній усім криптовалютам. Це досягається за допомогою забезпечення кожного коїна ліквідним матеріальним товаром або іншою криптовалютою. Також існують алгоритмічні стейблкоїни, які імітують монетарну політику фіатних валют.

Крім того, криптовалюти можна класифікувати за видом їхньої блокчейн платформи: приватні, публічні та гібридні.

Ми з’ясували, що використання технології блокчейн дозволяє криптовалютам виконувати наступні задачі: безпечні перекази, розрахунки без посередників. Ці особливості, наряду з швидшими транзакціями, роблять криптовалюти чудовим рішенням для міжнародних переказів. Також криптовалюти підходять для конфіденційних платежів та цифровізації активів. Конфіденційність та відсутність авторизації не означає, що криптовалюти підходять для фінансування незаконної діяльності. Завдяки тому, що біржі запрошують певні персональні дані при

реєстрації, ідентичність власника рахунка можна встановити. Станом на 2019 рік, лише 1% Біткоїну було використано у незаконних цілях.[50]

Дослідивши все вищезазначене, ми також дійшли до висновку, що криптовалюти виконують усі функції фіатних грошей, однак не мають однієї властивості – загального визнання. З кожним роком, усе більше країн вводять криптовалюти у якості ще одного платіжний засобу. Також ведеться розробка державних криптовалют або CBDC(Central Bank Digital Currency). Найбільш амбітним виглядає проєкт КНР - цифровий юань. Наразі технологія проходить етап активного тестування. Завдяки використанню розподіленої бази даних, досягається висока швидкість транзакції. Однак, на відміну від криптовалют, CBDC централізовані і контролюються державою. Влада Китаю переконана, що введення цифрового юаня дозволить краще контролювати та управляти грошовими масами, задля уникнення корупції та інфляції. [51]

На сьогоднішній день, в Україні немає законодавчого регулювання криптовалют і вони умовно знаходиться у “сірій” зоні – громадяни можуть ними користуватись, але покарання за протиправні дії, наприклад викрадення коїнів, не регламентовано жодною правовою нормою.

Криптовалюти та фіатні валюти мають зовсім різний принцип роботи, як з технічної точки зору, так і з точки зору економіки. Криптовалюти мають обмежену емісію, а отже, дефляційну природу. У той час як вартість фіатних валют має тенденцію до зниження, через збільшення грошої маси. Однак, обидва ці явища можуть бути корисними або катастрофічними, залежно від рівня. Нинішній економіці притаманна інфляція, але завдяки криптовалютам можуть з’явитись гібридні рішення, які дозволять зробити світову економіку більш стабільною та міцною.

Серед відмінностей можна також виділити коло осіб, які мають право створювати фіатні або криптовалюти. Цифрові гроші, на відміну від фіатних, може створювати будь-хто. Це дозволяє стимулювати та пришвидшити розвиток криптовалют: кожен охочий може продемонструвати власне удосконалення.

Оскільки коїни нічим не підкріплюються, то люди обирають куди інвестувати кошти виключно за рівнем довіри до криптовалюти та її технічним характеристикам.

Криптовалюти, хоч і виконують усі функції фіатних грошей, однак не можуть повністю їх замінити. Міжнародна фінансова система побудована на використанні фіатних валют.

Для створення криптовалюти було детально досліджено особливості різних видів цифрових грошей, стандарти та існуючі на ринку блокчейн платформи. Безпосередня розробка потребувала вивчення мови Solidity. Задля перевірки коректності роботи токена, було розглянуто засоби розгортання тестових мереж та особливості роботи з ними.

Розробка веб-застосунку вимагала отримання певної компетентності в роботі з інструментами, необхідними для безпосередньої побудови програми (Node.js, React, Bootstrap), та для розгортання смарт-контрактів і взаємодії з криптогаманцями (Web3, Truffle, Ganache, MetaMask, OneZeppelin). Більше того, було розглянуто NFT токени, їхні стандарти та особливості застосування.

Оскільки, було створено власну криптовалюту та веб-застосунок для роботи з NFT токенами, поставлена мета була успішно досягнута.

На мою думку, технологія блокчейн заслужила свою популярність і може з часом повністю витіснити деякі загальноприйняті рішення на ринку як у сфері економіки, так і державному управлінні. Створення криптовалют стало гарним поштовхом для розвитку фіатних грошей. Актуальні питання пришвидшення транзакцій, підвищення безпеки та конфіденційності стають наріжними каменями майбутніх змін.

## Список використаних джерел


1. How Does Blockchain Work? [Електронний ресурс] – https://academy.binance.com/en/articles/how-does-blockchain-work Дата доступу: 17.05.2021.
2. Antonopoulos A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1005 Gravenstein Highway North, Sebastopol : O'Reilly Media, Inc, 2014. 298 p.
3. What Is a Blockchain Consensus Algorithm? [Електронний ресурс] – https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm Дата доступу: 17.05.2021.
4. Обзор 9 алгоритмов блокчейн консенсуса [Електронний ресурс] – https://digiforest.io/blog/blockchain-consensus-algorithms Дата доступу: 17.05.2021.
5. What Is Proof of Work (PoW)? [Електронний ресурс] – https://academy.binance.com/en/articles/proof-of-work-explained Дата доступу: 17.05.2021.
6. Proof of Stake Explained [Електронний ресурс] – https://academy.binance.com/en/articles/proof-of-stake-explained Дата доступу: 17.05.2021.
7. Что такое Ethereum Casper? [Електронний ресурс] – https://academy.binance.com/ru/articles/ethereum-casper-explained Дата доступу: 17.05.2021.
8. Delegated Proof of Stake Explained [Електронний ресурс] – https://academy.binance.com/en/articles/delegated-proof-of-stake-explained Дата доступу: 17.05.2021.
9. Delegated Proof-of-Stake (DPoS) Explained [Електронний ресурс] – https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/ Дата доступу: 17.05.2021.

10. Proof of Capacity (Cryptocurrency) [Електронний ресурс] – https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp Дата доступу: 17.05.2021.
11. Proof-of-Capacity: Как это работает [Електронний ресурс] – https://ru.ihodl.com/tutorials/2018-04-18/proof-capacity-kak-eto-rabotaet/.
12. What is Chia? [Електронний ресурс] –https://www.chia.net/faq/ Дата доступу: 17.05.2021.
13. What Is Proof-of-Spacetime (PoSt)? [Електронний ресурс] – https://coinmarketcap.com/alexandria/glossary/proof-of-spacetime Дата доступу: 17.05.2021.
14. The great graphics card shortage of 2020 (and 2021) [Електронний ресурс] – https://www.bbc.com/news/technology-55755820 Дата доступу: 17.05.2021.
15. Майнеры Chia Coin спровоцировали дефицит жестких дисков в Гонконге [Електронний ресурс] – https://www.rbc.ru/crypto/news/607e924f9a79471665a36cf4 Дата доступу: 17.05.2021.
16. Proof of Activity [Електронний ресурс] – https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp Дата доступу: 17.05.2021.
17. Cryptocurrency Definition [Електронний ресурс] – https://www.investopedia.com/terms/c/cryptocurrency.asp Дата доступу: 17.05.2021.
18. Is Bitcoin Really Digital Gold? [Електронний ресурс] – https://www.forbes.com/sites/forbesfinancecouncil/2020/05/11/is-bitcoin-really-digital-gold/?sh=d73c0c62a842 Дата доступу: 17.05.2021.
19. Altcoin [Електронний ресурс] –https://academy.binance.com/en/glossary/altcoin Дата доступу: 17.05.2021.

20. What Is Bitcoin? [Електронний ресурс] – https://academy.binance.com/en/articles/what-is-bitcoin Дата доступу: 17.05.2021.
21. Bitcoin mining difficulty [Електронний ресурс] – https://data.bitcoinity.org/bitcoin/difficulty/all?t=l Дата доступу: 17.05.2021.
22. How It Works [Електронний ресурс] –https://z.cash/technology/ Дата доступу: 17.05.2021.
23. Что такое Monero? [Електронний ресурс] –https://forklog.com/chto-takoe-monero/ Дата доступу: 17.05.2021.
24. Как работают анонимные криптовалюты [Електронний ресурс] – https://www.rbc.ru/crypto/news/5d0b544c9a794722cc4524e3 Дата доступу: 17.05.2021.
25. What Are Stablecoins? [Електронний ресурс] – https://academy.binance.com/en/articles/what-are-stablecoins Дата доступу: 17.05.2021.
26. What Is Tether (USDT)? [Електронний ресурс] – https://academy.binance.com/en/articles/what-is-tether-usdt Дата доступу: 17.05.2021.
27. Private, Public, and Consortium Blockchains - What's the Difference? [Електронний ресурс] –https://academy.binance.com/en/articles/private-public-and-consortium-blockchains-whats-the-difference Дата доступу: 17.05.2021.
28. Where Blockchain Is Stored: Fundamentals Explained [Електронний ресурс] – https://101blockchains.com/where-blockchain-is-stored/ Дата доступу: 17.05.2021.
29. Токенизация активов и её влияние на финансовые рынки [Електронний ресурс] –https://digit.nsd.ru/articles/tokenizatsiya-aktivov-i-eye-vliyanie-na-finansovye-rynki/ Дата доступу: 17.05.2021.
30. WHAT IS TOKENIZATION? [Електронний ресурс] – https://coingeek.com/bitcoin101/what-is-tokenization/ Дата доступу: 17.05.2021.

31. An Introduction to ERC-20 Tokens [Електронний ресурс] – https://academy.binance.com/ru/articles/an-introduction-to-erc-20-tokens Дата доступу: 17.05.2021.
32. Больше, чем валюта. Зачем нужны токены стандарта ERC-20 [Електронний ресурс] – https://www.rbc.ru/crypto/news/601e6a409a79475871babe10 Дата доступу: 17.05.2021.
33. Crypto vs Visa: transactions' speed compared [Електронний ресурс] – https://payspacemagazine.com/cryptocurrency/crypto-vs-visa-transactions-speed-compared/ Дата доступу: 17.05.2021.
34. Правда ли, что криптовалюты — спасение от инфляции? [Електронний ресурс] – https://crypto-fox.ru/article/inflyatsiya-i-deflyatsiya-kriptovalyut/ Дата доступу: 17.05.2021.
35. Cryptocurrency Definition [Електронний ресурс] – https://www.financestrategists.com/finance-terms/cryptocurrency/ Дата доступу: 17.05.2021.
36. Что такое деньги [Електронний ресурс] – https://www.banki.ru/wikibank/dengi_wiki/ Дата доступу: 17.05.2021.
37. What Is The Fastest Blockchain And Why? Analysis of 43 Blockchains [Електронний ресурс] – https://alephzero.org/blog/what-is-the-fastest-blockchain-and-why-analysis-of-43-blockchains/ Дата доступу: 17.05.2021.
38. Regulation of Cryptocurrency Around the World [Електронний ресурс] – https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf Дата доступу: 17.05.2021.
39. Is Bitcoin a Store of Value? [Електронний ресурс] – https://academy.binance.com/en/articles/is-bitcoin-a-store-of-value.
40. Infographic: The Properties of Money [Електронний ресурс] – http://money.visualcapitalist.com/infographic-the-properties-of-money/ Дата доступу: 17.05.2021.

41. Qualities of Good Money [Електронний ресурс] – https://www.toppr.com/guides/business-economics-cs/money-and-banking/qualities-of-good-money/ Дата доступу: 17.05.2021.
42. What Is Fiat Currency? [Електронний ресурс] – https://academy.binance.com/en/articles/what-is-fiat-currency Дата доступу: 17.05.2021.
43. Биткоин вырос на 19% после изменений в Twitter Илона Маска [Електронний ресурс] – https://www.forbes.ru/newsroom/finansy-i-investicii/419867-bitkoin-vyros-na-19-posle-izmeneniy-v-twitter-ilona-maska Дата доступу: 17.05.2021.
44. Bitcoin price volatility [Електронний ресурс] – https://data.bitcoinity.org/markets/volatility/all/USD?c=e&f=m10&g=15&st=log&t=l Дата доступу: 17.05.2021.
45. Правда ли, что криптовалюты — спасение от инфляции? [Електронний ресурс] –https://crypto-fox.ru/article/inflyatsiya-i-deflyatsiya-kriptovalyut/ Дата доступу: 17.05.2021.
46. How to Create a Cryptocurrency: Everything You Need to Know [Електронний ресурс] –https://mlsdev.com/blog/how-to-create-your-own-cryptocurrency Дата доступу: 17.05.2021.
47. UNDERSTAND THE ERC-20 TOKEN SMART CONTRACT [Електронний ресурс] –https://ethereum.org/en/developers/tutorials/understand-the-erc-20-token-smart-contract/ Дата доступу: 17.05.2021.
48. Non-fungible Token (NFT) [Електронний ресурс] – Режим доступу до ресурсу: https://academy.binance.com/ru/glossary/non-fungible-token-nft Дата доступу: 17.05.2021.
49. Developer Survey [Електронний ресурс] – Режим доступу до ресурсу: https://insights.stackoverflow.com/survey/2020#technology-most-loved-dreaded-and-wanted-other-frameworks-libraries-and-tools-wanted3 Дата доступу: 17.05.2021.

50. 1% Bitcoin использовался в незаконных целях в 2019 году [Електронний ресурс] – https://www.rbc.ru/crypto/news/5d1ccb1d9a794773561c0c2c Дата доступу: 17.05.2021.
51. Китай рассказал об итогах тестирования цифрового юаня [Електронний ресурс] – https://www.rbc.ru/crypto/news/5f8d83a69a7947976d8dc9ee Дата доступу: 17.05.2021.